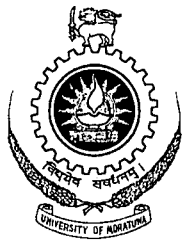

SUPPLY CHAIN MANAGEMENT and its RESPONSE to TERRORISM in SRI LANKAN APPAREL SECTOR

By

Captain N Kuruparan

Supervised by

Dr P.Ramachandran

This dissertation was submitted to the Department of Management of Technology of the University of Moratuwa in partial fulfillment of the requirement for the degree of Master of Business Administration in Management of Technology

Department of Management of Technology

University of Moratuwa

November 2006

DECLARATION

I hereby certify that this dissertation entitled "Supply Chain Management & it's Response to Terrorism In Sri Lankan Apparel Sector" is entirely my own work and it has never been submitted nor is it currently being submitted for any other degree. I also hereby give consent for my dissertation, if accepted, to be made available for photocopying and for interlibrary loans, and for the title and summary to be made available to outside organization.

..... Date: 31st Jan 2007

N Kuruparan

Captain – Sri Lanka Navy

..... Date: 2nd Feb 2007

Dr. P Ramachandran

CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATION

LIST OF ABREVIATIONS

SCM	Supply Chain Management
DoD	Department of Defence
CTPAT	Custom-Trade Partnership Against Terrorism
USA	United States of America
EU	European Union
OEM	Original Equipment Manufacturers
SCOR	Supply Chain Operations Reference Model
SARS	Severe Acute Respiratory Syndrome
OSC	Op-Safe Commerce
CSI	Container Security Initiative
FAST	Free and Secure Trade
RFID	Radio Frequency Identification
VMI	Vendor Manage Inventory
CMI	Customer Managed Inventory
JIT	Just in Time
CPFR	Collaborative Planning, Forecasting and Replenishment
PEST	Political, Economic, Social and Technological
SCEM	Supply Chain Event Management
TQM	Total Quality Management
IT	Information Technology
IS	Information System
B2B	Business to Business
OS&D	Overages, Shortages, and Damages
SKU	Stores Keeping Unit

ACKNOWLEDGEMENT

I would like to take this opportunity to express my sincere thanks to Dr. P Ramachnadran Senior Lecturer Department of management of Technology (Project Supervisor) for his in valuable advice, understanding and encouragement given to me during this study. I would like to thank Dr. HSC Perera (Head of Department of Management of Technology), Dr Mrs V. Wickramasinghe, Mr Raj Prasana (Course Coordinator) for their timely guidance invaluable advice and support given through out the project.

I also with to thank the senior management of apparel sector companies for their valuable inputs and support during the project.

I wish to express my appreciation to the Sri Lanka Navy and in particular Commodore JC Hettigama, Director General, Electrical and Electronic Engineering Directorate for permitting me to follow the course.

I would also like to express my gratitude to the staff at Department of Management of Technology for valuable assistance rendered to me. Finally I would like to thank the Management of Technology faculty and all my colleagues who helped me to carry out this study and make it a success.

Finally, I lovingly and gratefully thank my beloved wife and children in helping and supporting my efforts to produce this research paper. Their sacrifice in fulfilling my ambition is appreciated.

ABSTRACT

The opening chapter dwells on how supply chain managers became aware of a new operating environment after the terrorist attacks on the World Trade Centre and the Pentagon on September 11, 2001. These events exposed the pre-existing and latent risk of disruption to supply networks from terrorist attacks. The risk was there all along but the attacks brought home the reality and the sheer vulnerability in everyone's minds. Sri Lanka is not different to USA. The country faces terrorist attacks to its infrastructure, business interests and key financial institutes such as the Central Bank of Sri Lanka. Furthermore, these events began to expose the total interdependence that exists between all firms in the supply network. The interdependence also includes reliance on those Sri Lankan Government agencies involved with inbound and outbound material flows and transportation infrastructure. Given these interdependencies, if one firm fails in the supply network, the entire network performance is at risk. Understandably, this constitutes a new operating environment where firms need to think in terms of their supply network and not just their individual performance.

The new operating environment calls for designing security and building resilience into the supply network. Security and resilience are unique characteristics that require distinct plans in order to develop and create these characteristics within the firm. Fortunately, there are several actions that firms can take which will contribute to both improved security and resilience. Improvement in security does not guarantee resilience. Neither does the addressing of resilience issues bring about security. The experience is that it is critical to design for both security and resilience.

New organizational capabilities are also called for in this environment. Specifically, firms will need to pioneer new relationships with Government agencies that now share responsibility for making the supply network secure and resilient. Additionally, firms will need to develop deeper relationships with suppliers and customers in their supply networks to jointly build a more secure and resilient network. Internally the largest organizational challenge may be in establishing at the individual level, a solid understanding of the interdependence of the systems, and the educational and training systems needed for robust network designs and

planned responses to disruptions. The Centre for Transportation and Logistics and the School of Management of Cranfield University prepared a practical guide and self assessment to understand the supply chain risks. This develops into the response to terrorist attacks and the change in the operating environment.

Redundancy, flexibility, vulnerability, visibility, velocity, acceleration, Collaborative planning and agility relationship are identified and extracted through an extensive literature survey described in chapter 2.

Chapter 3 describes the methodology of the research and the data and information collation procedures.

Past, present and future Corporate, Government and insurance industry responses to the terrorist disruption and natural disasters are identified. Also the risk identification methodologies, mapping risk, risk assessment and identifying benefits are discussed. The role of technology (Risk identification, analysis and mitigation) is also discussed in chapter 4.

"Ultimately, you need to tie risk (of attack, disruption) to business performance." Chapter 5 expands on these insights and builds a useful foundation for managers to use in designing their response in anticipation of future inevitable disruptions to the supply network by terrorism.

The final chapter lists the steps to reduce vulnerability, its justification and setting up of Distribution Response Centre.